UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/043,388	10/26/2001	Raymond Krasinski	US 010556	4672

24737 7590 05/04/2005

PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
WILLIAMS, JEFFERY L	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 05/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/043,388	KRASINSKI ET AL.	
	Examiner	Art Unit	
	Jeffery Williams	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 October 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10-26-01* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *10-26-01, 1-26-04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 19 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 19 recites the limitation, "wherein only the random or pseudo-random number is stored within the device." However, this claim depends upon claim 16, and therefore, requires the limitations of "at least one preselected unique or distinctive hardware, software or firmware identifier" contained within the device, and the forming of a key derived from a combination of the "random or pseudo-random number" and the "at least one preselected unique or distinctive" identifier(s). The limitation of claim 19 creates confusion as to how the key is formed if there were not present "at least one preselected unique or distinctive hardware, software or firmware identifier within the device". It is uncertain as to the proper interpretation of the limitations of claim 19, and it would not be proper to reject the claim on the basis of prior art (see in In re Steele, 305 F.2d 859,134 USPQ 292 (CCPA 1962)).

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 16 – 20 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Regarding claim 16, it is addressed to a key comprised of two data portions. The key is non-functional descriptive material, directed to data, *per se*. The key does not constitute a data structure, since there is no claimed functional interrelationship between data elements. Further, the key, introduced in the preamble, is "transmitted within a signal", therefore, claim 16 is also rejected as not being tangibly embodied because a signal is not tangible.

Regarding claims 17 – 20, they are rejected since they do not further modify claim 16 so as to become statutory.

For the purposes of searching prior art, it is presumed that the applicant will place claims 16 – 20 within a statutory category.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

Claims 1, 2, 4 – 8, and 10 are rejected under 35 U.S.C. 102(a) as being anticipated by Hales et al., "Method and System for Securely Downloading Content to Users", International Patent, WO 01/79971 A. Regarding these claims, they are rejected for the reasons supplied by the European patent examiner in the International Search Report performed on 12/19/03.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1 – 18 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Iverson, "Making the Internet Safe for the Music Industry" in view of Mizikovsky et al., Automatic Generation of Private

Authentication Key for Wireless Communication Systems", U.S. Patent 5,513,245.

Regarding claim 1, the applicant has disclosed as prior art the existence of the Secure Digital Music Initiative (SDMI). SDMI defines a domain or system "intended to prevent unauthorized copying of digital music", comprising software (applications and modules) and hardware (portable devices and media). It is alleged that a person might somehow be able to circumvent the copy protection of the SDMI standard because the software domain is not bound to the hardware domain (The instant application, page 1, "Background of the Invention"). To address this problem, the applicant discloses "a method of binding copy protection program for securely holding the digital content to particular device via a key derived in part from unique or distinctive hardware, software and/or firmware identifiers within the device and in part from a random or pseudo-random number (The instant application, page 3, "Summary of the Invention", lines 6-11). Iverson discloses a system according to the Secure Digital Music Initiative (SDMI) specifications (Iverson, par. 2). The disclosed system employs a method of copy protection by binding the software domain to the hardware domain. In other words, the proper execution of the content managing software/firmware of a device depends upon the existence of unique hardware and firmware identifiers contained within the device. The key is derived from a plurality of hardware/firmware identifiers (Iverson, pars. 5, 6). Thus, Iverson discloses a copy protection program to securely hold protected content and

validates a device when a key is used to access the protected content (Iverson, par. 5, lines 4,5). The key is used to validate (authenticate) the device so as to gain access to protected content. As stated by the applicant, the derivation of the key from a plurality of unique device identifiers contributes to the distinctive linking of the key to the device (The instant application, page 9, lines 20-24; page 10, lines 13-20). The applicant further discloses that the addition of the random number element to the key, protects the key by further adding to the uniqueness of the key (The instant application, page 10, line 21 – page 11, line 4). Thus, someone with the intent on illegally gaining access to protected content could not generate the key simply by "making a binary copy of the SDMI domain" and then distribute "the copies inappropriately to others" (The instant application, page 2, lines 2-5). Iverson does not disclose that the key is derived in part from a random or pseudo-random number.

However, adding a random number element to a key so as to make an unique authentication key for a device it is well known in the art. Mizikovsky et al. discloses that an authentication key used to validate a mobile device can be derived in part from distinctive hardware identifiers found within the device and in part from a random number received by the device (Mizikovsky et al, Abstract; col. 1, lines 28-45). Mizikovsky et al. discloses that it is advantageous to add the random number element to the key because, otherwise, unauthorized persons could illegally generated the authentication key and gain access to a protected system simply by making a copy of the unique identifiers found within the device (Mizikovsky et al., col. 1, lines 46-67). Mizikovsky shows that it is possible for

device identifiers to be stolen, and that authentication keys derived solely from the device identifiers are compromised. Thus, Mizikovsky et al. discloses a method of creating an authentication key derived in part from unique identifiers within a device and in part from a random number received by the device.

It would have been obvious to one of ordinary skill in the art to combine the method Mizikovsky et al. for generating a unique and more secure authentication key with the system and method of Iverson for gaining access to protected content through the use of a unique authentication key because it is obvious that an authentication key derived in part from a random number element received by the device could help prevent the illegal generation of the key through the copying of the hardware environment. Thus, the combination of Iverson and Mizikovsky et al. discloses the generation of a key derived in part from a least one preselected unique identifier found within the device and in part from a random number.

Regarding claim 2, the combination of Iverson and Mizikovsky et al., discloses:

accessing a value within the device for least one preselected hardware, software or identifier; firmware identifier (Iverson, par. 6.; Mizikovsky et al., col. 2, lines 3-14).

retrieving a stored value relating to the key from a storage location within the device (Iverson, par. 6.; Mizikovsky et al., col. 2, lines 3-14).

computing value for the key from the accessed value for the at least one preselected hardware, software or firmware identifier and the stored value relating to the key (Iverson, par. 6.; Mizikovsky et al., col. 2, lines 3-14).

and at least one of: controlling access to the protected content based upon a comparison of the computed value for the key and the stored value relating the key; and employing the computed value for the key to decrypt the protected content (Iverson, pars. 5, 6).

Regarding claim 3, the combination of Iverson and Mizikovsky et al. discloses:

wherein the key is derived in part from a plurality of preselected unique or distinctive hardware, software or firmware identifiers within the device (Iverson, par. 6).

Regarding claim 4, the combination of Iverson and Mizikovsky et al. discloses:

wherein the key is employed to control access to the protected content without being employed to encrypt or decrypt the protected content, thereby allowing the protected content be copied or transferred from the device to another device (Iverson, pars. 5, 6). As disclosed by Iverson, the key is used to boot the device, thus allowing access to the content.

Regarding claim 5, the combination of Iverson and Mizikovsky et al. discloses:

wherein the stored value relating to the key contains only the random or pseudo-random number (Mizikovsky et al., col. 1, lines 31-35). According to claim 2, the stored value is the random number received by the device. As disclosed by the combination of Iverson and Mizikovsky et al., the stored value contains the random number received by the device.

Regarding claim 6, the combination of Iverson and Mizikovsky et al. discloses:

at least one hardware, software, firmware component within the device having associated therewith a unique or distinctive identifier (Iverson, par. 6);

and copy protection program selectively executable within the device and securely holding the protected content, wherein the copy protection program, when employed to access the protected content, validates the device based upon a key derived part from the identifier for the least one hardware, software or firmware component and in part from a random or pseudo-random number (Iverson, pars. 5, 6).

Regarding claims 7 – 10, they are the device claims corresponding to the system claims 2 – 5 and they are rejected for the same reasons.

Regarding claims 11 – 15, they are the method claims with the corresponding limitations of the device claims 6 – 10 and they are rejected for the same reasons.

Regarding claim 16, the combination of Iverson and Mizikovsky et al. disclose a key comprising:

a first portion derived from at least one unique or distinctive hardware, software or firmware identifier within the device (Iverson, par. 6.; Mizikovsky et al., col. 2, lines 3-14).

and a second portion derived from a random or pseudo-random number (Mizikovsky et al., col. 2, lines 3-14).

wherein the key is employed by a copy protection program securely holding protected content within the device to validate device when employed to access the protected content (Iverson, par 5, lines 3-5).

Regarding claims 17 and 18, they are apparatus claims corresponding to the system claims 3 and 4 and they are rejected for the same reasons.

Regarding claim 20, the combination of Iverson and Mizikovsky et al. disclose:

wherein only the random or pseudo-random number transmitted within the signal to the device (Mizikovsky et al., col. 2, lines 6-8).

.

Claim 3 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hales et al., "Method and System for Securely Downloading Content to Users", International Patent, WO 01/79971 A in view of Joshi, "Computer Software Security System", U.S. Patent, 4,688,169. Claims 3 and 9 are rejected for the reasons supplied by the European patent examiner in the International Search Report performed on 12/19/03.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

Cok, "System for Secure Distribution and Playback of Digital Data", U.S. Patent 6,865,550 B1.

Sims, III, "Media Content Protection Utilizing Public Key Cryptography", U.S. Patent 6,550,011 B1.

Kataoka et al.; "Security System for Protecting Information Stored in Portable Storage Media", U.S. Patent 5,857,021.

Lee et al., "System for Preventing an Illegal Copy of Digital Contents", European Patent, EP 1051011 A2.

Jon Iverson, "Making the Internet Safe for the Music Industry", 3/5/2000, Stereophile, www.stereophile,com/news/10691/index.html.

Business Wire/Gale Group, "Cirrus Logic and InterTrust Launch hardware/Software Solution That Enables Secure Internet Distribution for Billion-Dollar Music Industry", 3/2/2000, www.looksmart.com.

Matt Perry, "Ensuring Security the Hard Way", 12/01/2000, EETimes Online.

"Is SDMI a Consumer's Nightmare?", 2/3/2000, Slashdot, http://slashdot.org/article.pl?sid=00/02/02/1124200&mode=nested.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffery Williams whose telephone number is (571) 272-7965. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jeffery Williams
571.272.7965
4.27.05

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER